UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. LORI DREW, Defendant.	No. CR 08-0582-GW DECISION ON DEFENDANT'S F.R.CRIM.P. 29(c) MOTION

I. INTRODUCTION

This case raises the issue of whether (and/or when will) violations of an Internet website's[1] terms of service constitute a crime under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Originally, the question arose in the context of Defendant Lori Drew's motions to dismiss the Indictment on grounds of vagueness, failure to state an offense, and unconstitutional delegation of prosecutorial power. See Case Docket Document Numbers ("Doc. Nos.") 21, 22, and 23. At that time, this Court found that the presence of the scienter element (i.e. the requirement that the intentional accessing of a computer without authorization or in excess of authorization

[1] There is some disagreement as to whether the words "Internet" and "website" should be capitalized and whether the latter should be two words (i.e. "web site") or one. "Internet" is capitalized as that is how the word appears most often in Supreme Court opinions. See, e.g., Pac. Bell Tel. Co. v. linkline Comms., Inc., 555 U.S. ___, 129 S.Ct. 1109, 1115 (2009).

be in furtherance of the commission of a criminal or tortious act) within the CFAA felony provision as delineated in 18 U.S.C. § 1030(c)(2)(B)(ii) overcame Defendant's constitutional challenges and arguments against the criminalization of breaches of contract involving the use of computers. See Reporter's Transcripts of Hearings on September 4 and October 30, 2008. However, Drew was subsequently acquitted by a jury of the felony CFAA counts but convicted of misdemeanor CFAA violations. Hence, the question in the present motion under Federal Rule of Criminal Procedure ("F.R.Crim.P.") 29(c) is whether an intentional breach of an Internet website's terms of service, without more, is sufficient to constitute a misdemeanor violation of the CFAA; and, if so, would the statute, as so interpreted, survive constitutional challenges on the grounds of vagueness and related doctrines.[2]

II. BACKGROUND

A. Indictment

In the Indictment, Drew was charged with one count of conspiracy in violation of 18 U.S.C. § 371 and three counts of violating a felony portion of the CFAA, i.e., 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), which prohibit accessing a computer without authorization or in excess of authorization and obtaining information

---

[2] While this case has been characterized as a prosecution based upon purported "cyberbulling," there is nothing in the legislative history of the CFAA which suggests that Congress ever envisioned such an application of the statute. See generally, A. Hugh Scott & Kathleen Shields, Computer and Intellectual Property Crime: Federal and State Law (2006 Cumulative Supplement) 4-8 to 4-16 (BNA Books 2006). As observed in Charles Doyle & Alyssa Weir, CRS Report for Congress - Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws (Order Code 97-1025) (Updated June 28, 2005):

> The federal computer fraud and abuse statute, 18 U.S.C. 1030, protects computers in which there is a federal interest – federal computers, bank computers, and computers used in interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, instead it fills cracks and gaps in the protection afforded by other state and federal criminal laws.

Moreover, once Drew was acquitted by the jury of unauthorized accessing of a protected computer in furtherance of the commission of acts of intentional infliction of emotional distress, this case was no longer about "cyberbulling" (if, indeed, it was ever properly characterized as such); but, rather, it concerned the proper scope of the application of the CFAA in the context of violations of a website's terms of service.

from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime or tortious act. See Doc. No. 1.

The Indictment included, inter alia, the following allegations (not all of which were established by the evidence at trial). Drew, a resident of O'Fallon, Missouri, entered into a conspiracy in which its members agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress[3] upon "M.T.M.," subsequently identified as Megan Meier ("Megan"). Megan was a 13 year old girl living in O'Fallon who had been a classmate of Drew's daughter Sarah. Id. at ¶¶ 1- 2, 14. Pursuant to the conspiracy, on or about September 20, 2006, the conspirators registered and set up a profile for a fictitious 16 year old male juvenile named "Josh Evans" on the www.MySpace.com website ("MySpace"), and posted a photograph of a boy without that boy's knowledge or consent. Id. at ¶ 16. Such conduct violated MySpace's terms of service. The conspirators contacted Megan through the MySpace network (on which she had her own profile) using the Josh Evans pseudonym and began to flirt with her over a number of days. Id. On or about October 7, 2006, the conspirators had "Josh" inform Megan that he was moving away. Id. On or about October 16, 2006, the conspirators had "Josh" tell Megan that he no longer liked her and that "the world would be a better place without her in it." Id. Later on that same day, after learning that Megan had killed herself, Drew caused the Josh Evans MySpace account to be deleted. Id.

---

[3] The elements of the tort of intentional infliction of emotional distress are the same under both Missouri and California state laws. Those elements are: (1) the defendant must act intentionally or recklessly; (2) the defendant's conduct must be extreme or outrageous; and (3) the conduct must be the cause (4) of extreme emotional distress. See, e.g., Thomas v. Special Olympics Missouri, Inc., 31 S.W.3d 442, 446 (Mo. Ct. App. 2000); Hailey v. California Physicians' Service, 158 Cal.App.4th 452, 473-74 (2007).

B. Verdict

At the trial, after consultation between counsel and the Court, the jury was instructed that, if they unanimously decided that they were not convinced beyond a reasonable doubt as to the Defendant's guilt as to the felony CFAA violations of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), they could then consider whether the Defendant was guilty of the "lesser included"[4] misdemeanor CFAA violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A).[5]

At the end of the trial, the jury was deadlocked and was unable to reach a verdict as to the Count 1 conspiracy charge.[6] See Doc. Nos. 105 and 120. As to Counts 2 through 4, the jury unanimously found the Defendant "not guilty" "of [on

---

[4] As provided in F.R.Crim.P. 31(c)(1), a "defendant may be found guilty of . . . an offense necessarily included in the offense charged . . . ." A "lesser included" crime is one where "the elements of the lesser offense are a subset of the elements of the charged offense." Carter v. United States, 530 U.S. 255, 260 (2000) (quoting Schmuck v. United States, 489 U.S. 705, 716 (1989)). Because the felony CFAA crime in 18 U.S.C. § 1030(c)(2)(B)(ii) consists of committing acts which constitute a violation of the misdemeanor CFAA crime in 18 U.S.C. § 1030(a)(2)(C) (as delineated in 18 U.S.C. § 1030(c)(2)(A)) plus the additional element that the acts were done "in furtherance of any crime or tortious act in violation of the Constitution or laws of the United States or any State," the misdemeanor CFAA crime is a "lesser included" offense as to the felony CFAA violation.

A defendant is entitled to a "lesser included" offense jury instruction if the evidence warrants it. Guam v. Fejeran, 687 F.2d 302, 305 (9th Cir. 1982).

[5] Specifically, the jury was instructed that:

> The crime of accessing a protected computer without authorization or in excess of authorization to obtain information, and to do so in furtherance of a tortious act in violation of the laws of any State, includes the lesser crime of accessing a protected computer without authorization or in excess of authorization. If (1) all of you are not convinced beyond a reasonable doubt that the defendant is guilty of accessing a protected computer without authorization or in excess of authorization to obtain information, and doing so in furtherance of a tortious act in violation of the laws of any State; and (2) all of you are convinced beyond a reasonable doubt that the defendant is guilty of the lesser crime of accessing a protected computer without authorization or in excess of authorization, you may find the defendant guilty of accessing a protected computer without authorization or in excess of authorization.

See Jury Instruction No. 24, Doc. No. 107.

[6] The conspiracy count was subsequently dismissed without prejudice at the request of the Government.

the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in furtherance of the tort of intentional infliction of emotional distress in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(ii) . . . ." Id. The jury did find Defendant "guilty" "of [on the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor." Id.

C. MySpace.com

As Jae Sung (Vice President of Customer Care at MySpace) ("Sung") testified at trial, MySpace is a "social networking" website where members can create "profiles" and interact with other members. See Reporter's Transcript of the November 21, 2008 Sung testimony ("11/21/08 Transcript") at pages 40-41. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles which are not set as "private." Id. at 42. However, to create a profile, upload and display photographs, communicate with persons on the site, write "blogs," and/or utilize other services or applications on the MySpace website, one must be a "member." Id. at 42-43. Anyone can become a member of MySpace at no charge so long as they meet a minimum age requirement and register. Id.

In 2006, to become a member, one had to go to the sign-up section of the MySpace website and register by filling in personal information (such as name, email address, date of birth, country/state/postal code, and gender) and creating a password. Id. at 44-45. In addition, the individual had to check on the box indicating that "You agree to the MySpace **Terms of Service** and **Privacy Policy**." See Government's[7]

[7] All exhibits referenced herein were proffered by the Government and admitted during the trial.

Exhibit 1 at page 2 (emphasis in original); 11/21/08 Transcript at 45-47. The terms of service did not appear on the same registration page that contained this "check box" for users to confirm their agreement to those provisions. Id. In order to find the terms of service, one had (or would have had) to proceed to the bottom of the page where there were several "hyperlinks" including one entitled "Terms." 11/21/08 Transcript at 50; Exhibit 1 at 5. Upon clicking the "Terms" hyperlink, the screen would display the terms of service section of the website. Id. A person could become a MySpace member without ever reading or otherwise becoming aware of the provisions and conditions of the MySpace terms of service by merely clicking on the "check box" and then the "Sign Up" button without first accessing the "Terms" section. 11/21/08 Transcript at 94.[8]

As used in its website, "terms of service" refers to the "MySpace.com Terms of Use Agreement" ("MSTOS"). See Government's Exhibit 3. The MSTOS in 2006 stated, inter alia:

> This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the Services. By using the Services, you agree to be bound by this Agreement, whether you are a "Visitor" (which means that you simply browse the Website) or you are a "Member" (which means that you have registered with Myspace.com). The term "User" refers to a Visitor or a Member. You are only authorized to use the Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the Website and discontinue use of the Services immediately. If you wish to become a Member, communicate with other Members and make use of the Services, you must read this Agreement and indicate your acceptance at the end of this document before proceeding.

Id. at 1.

---

[8] Certain websites endeavor to compel visitors to read their terms of service by requiring them to scroll down through such terms before being allowed to click on the sign-on box or by placing the box at the end of the "terms" section of the site. Id. at 93. MySpace did not have such provisions in 2006. Id. See generally Southwest Airlines, Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 at *13-16 & n.4 (N.D. Tex. 2007) (discussing various methods that websites employ to notify users of terms of service).

> By using the Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the Services does not violate any applicable law or regulation.

Id. at 2.

The MSTOS prohibited the posting of a wide range of content on the website including (but not limited to) material that: a) "is potentially offensive and promotes racism, bigotry, hatred or physical harm of any kind against any group or individual"; b) "harasses or advocates harassment of another person"; c) "solicits personal information from anyone under 18"; d) "provides information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous"; e) "includes a photograph of another person that you have posted without that person's consent"; f) "involves commercial activities and/or sales without our prior written consent"; g) "contains restricted or password only access pages or hidden pages or images"; or h) "provides any phone numbers, street addresses, last names, URLs or email addresses . . . ." Id. at 4. MySpace also reserved the right to take appropriate legal action (including reporting the violating conduct to law enforcement authorities) against persons who engaged in "prohibited activity" which was defined as including, inter alia: a) "criminal or tortious activity", b) "attempting to impersonate another Member or person", c) "using any information obtained from the Services in order to harass, abuse, or harm another person", d) "using the Service in a manner inconsistent with any and all applicable laws and regulations", e) "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services", f) "selling or otherwise transferring your profile", or g) "covering or obscuring the banner advertisements on your personal profile page . . . ." Id. at 5. The MSTOS warned users that "information provided by other MySpace.com Members (for instance, in their Profile) may contain inaccurate, inappropriate, offensive or sexually explicit material, products or services, and MySpace.com assumes no responsibility or liability for this material." Id. at 1-2.

Further, MySpace was allowed to unilaterally modify the terms of service, with such modifications taking effect upon the posting of notice on its website. Id. at 1. Thus, members would have to review the MSTOS each time they logged on to the website, to ensure that they were aware of any updates in order to avoid violating some new provision of the terms of service. Also, the MSTOS provided that "any dispute" between a visitor/member and MySpace "arising out of this Agreement must be settled by arbitration" if demanded by either party. Id. at 7.

At one point, MySpace was receiving an estimated 230,000 new accounts per day and eventually the number of profiles exceeded 400 million with over 100 million unique visitors worldwide. 11/21/08 Transcript at 74-75. "Generally speaking," MySpace would not monitor new accounts to determine if they complied with the terms of service except on a limited basis, mostly in regards to photographic content. Id. at 75. Sung testified that there is no way to determine how many of the 400 million existing MySpace accounts were created in a way that violated the MSTOS.[9] Id. at 82-84. The MySpace website did have hyperlinks labelled "Safety Tips" (which contained advice regarding personal, private and financial security vis-a-vis the site) and "Report Abuse" (which allowed users to notify MySpace as to inappropriate content and/or behavior on the site). Id. at 51-52. MySpace attempts to maintain adherence to its terms of service. Id. at 60. It has different teams working in various areas such as "parent care" (responding to parents' questions about this site), handling "harassment/cyberbully cases, imposter profiles," removing inappropriate content, searching for underage users, etc. Id. at 60-61. As to MySpace's response to reports

---

[9] As stated in the MSTOS:

> MySpace.com does not endorse and has no control over the Content. Content is not necessarily reviewed by MySpace.com prior to posting and does not necessarily reflect the opinions or policies of MySpace.com. MySpace.com makes no warranties, express or implied, as to the Content or to the accuracy and reliability of the Content or any material or information that you transmit to other Members.

Exhibit 3 at 3.

of harassment:

> It varies depending on the situation and what's being reported. It can range from . . . letting the user know that if they feel threatened to contact law enforcement, to us removing the profile, and in rare circumstances we would actually contact law enforcement ourselves.

Id. at 61.

Once a member is registered and creates his or her profile, the data is housed on computer servers which are located in Los Angeles County. Id. at 53. Members can create messages which can be sent to other MySpace members, but messages cannot be sent to or from other Internet service providers such as Yahoo!. Id. at 54. All communications among MySpace members are routed from the sender's computer through the MySpace servers in Los Angeles. Id. at 54-55.

Profiles created by adult MySpace members are by default available to any user who accesses the MySpace website. Id. at 56. The adult members can, however, place privacy settings on their accounts such that only pre-authorized "friends" are able to view the members' profile pages and contents. Id. For members over 16 but under 18, their profiles are by default set at "private" but can be changed by the member. Id. at 57. Members under 16 have a privacy setting for their profiles which cannot be altered to allow regular public access. Id. To communicate with a member whose profile has a privacy setting, one must initially send a "friend" request to that person who would have to accept the request. Id. at 57-58. To become a "friend" of a person under 16, one must not only send a "friend" request but must also know his or her email address or last name. Id. at 58.

According to Sung, MySpace owns the data contained in the profiles and the other content on the website.[10] MySpace is owned by Fox Interactive Media which

---

[10] Technically, as delineated in the MSTOS, Exhibit 3 at pages 2-3:

> By displaying or publishing ("posting") any Content, messages, text, files, images, photos, video, sounds, profiles, works or authorship, or any other materials (collectively, "Content") on or through the Services, you hereby

is part of News Corporation. Id. at 42.

III. APPLICABLE LAW

A. F.R.Crim.P. 29(c)

A motion for judgment of acquittal under F.R.Crim.P. 29(c) may be made by a defendant seeking to challenge a conviction on the basis of the sufficiency of the evidence, see, e.g., United States v. Freter, 31 F.3d 783, 785 (9th Cir. 1994), or on other grounds including ones involving issues of law for the court to decide, see, e.g. United States v. Pardue, 983 F.2d 843, 847 (8th Cir. 1993) (issue as to whether a defendant is entitled to a judgment of acquittal based on outrageous government conduct is "one of law for the court"). Where the Rule 29(c) motion rests in whole or in part on the sufficiency of the evidence, the evidence must be viewed "in the light most favorable to the government" (see Freter, 31 F.3d at 785), with circumstantial evidence and inferences drawn in support of the jury's verdict. See United States v. Lewis, 787 F.2d 1318, 1323 (9th Cir. 1986).

B. The CFAA

In 2006, the CFAA (18 U.S.C. § 1030) provided in relevant part that:

> (a) Whoever –
> * * * *
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

---

grant to MySpace.com, a non-exclusive, fully-paid and royalty-free, worldwide license (with the right to sublicense through unlimited levels of sublicensees) to use, copy, modify, adapt, translate, publicly perform, publicly display, store, reproduce, transmit, and distribute such Content on and through the Services. This license will terminate at the time you remove such Content from the Services. Notwithstanding the foregoing, a back-up or residual copy of the Content posted by you may remain on the MySpace.com servers after you have removed the Content from the Services, and MySpace.com retains the rights to those copies.

> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer if the conduct involved an interstate or foreign communication;[11]
>
> * * * *
>
> shall be punished as provided in subsection (c) of this section.
>
> * * * *
>
> (c) The punishment for an offense under subsection (a) or (b) of this section is –
>
> * * * *
>
> (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; . . .
>
> (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if –
>
> (i) the offense was committed for purposes of commercial advantage or private financial gain;
>
> (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
>
> (iii) the value of the information obtained exceeds $5,000 . . . .

As used in the CFAA, the term "computer" "includes any data storage facility or communication facility directly related to or operating in conjunction with such device . . . ." 18 U.S.C. § 1030(e)(1). The term "protected computer" "means a computer - (A) exclusively for the use of a financial institution or the United States Government . . . ; or (B) which is used in interstate or foreign commerce or communication . . . ." Id. § 1030(e)(2). The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . .

---

[11] On September 26, 2008, the Identity Theft Enforcement and Restitution Act of 2008 was passed which amended 18 U.S.C. § 1030(a)(2)(C) by inter alia striking the words "if the conduct involved an interstate or foreign communication" after "protected computer." See 110 P.L. 326, Title II, § 203, 112 Stat. 3560-65.

." Id. § 1030(e)(6).

In addition to providing criminal penalties for computer fraud and abuse, the CFAA also states that "[A]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). Because of the availability of civil remedies, much of the law as to the meaning and scope of the CFAA has been developed in the context of civil cases.

IV. DISCUSSION

A. The Misdemeanor 18 U.S.C. § 1030(a)(2)(C) Crime Based on Violation of a Website's Terms of Service

During the relevant time period herein,[12] the misdemeanor 18 U.S.C. § 1030(a)(2)(C) crime consisted of the following three elements:

> First, the defendant intentionally [accessed without authorization] [exceeded authorized access of] a computer;
>
> Second, the defendant's access of the computer involved an interstate or foreign communication; and
>
> Third, by [accessing without authorization] [exceeding authorized access to] a computer, the defendant obtained information from a computer . . . [used in interstate or foreign commerce or communication] . . . .

Ninth Circuit Model Criminal Jury Instruction 8.79 (2003 Ed.) (brackets in original).

In this case, a central question is whether a computer user's intentional violation of one or more provisions in an Internet website's terms of services (where those terms condition access to and/or use of the website's services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C). If the answer to that question is "yes," then seemingly, any and every conscious violation of that website's terms of service will constitute a CFAA misdemeanor.

Initially, it is noted that the latter two elements of the section 1030(a)(2)(C)

---

[12] See footnote 11, supra.

crime will always be met when an individual using a computer contacts or communicates with an Internet website. Addressing them in reverse order, the third element requires "obtain[ing] information" from a "protected computer" - which is defined in 18 U.S.C. § 1030(e)(2)(B) as a computer "which is used in interstate or foreign commerce or communication . . . ." "Obtain[ing] information from a computer" has been described as "'includ[ing] mere observation of the data. Actual aspiration . . . need not be proved in order to establish a violation . . . .' S.Rep. No. 99-432, at 6-7 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2484." Comment, Ninth Circuit Model Criminal Instructions 8.77.[13] As for the "interstate or foreign commerce or communication" component, the Supreme Court in Reno v. American Civil Liberties Union, 521 U.S. 844, 849 (1997), observed that: "The Internet is an international network of interconnected computers." See also Brookfield Communications v. West Coast Entertainment Corp., 174 F.3d 1036, 1044 (9th Cir. 1999) ("The Internet is a global network of interconnected computers which allows individuals and organizations around the world to communicate and to share information with one another."). The Ninth Circuit in United States v. Sutcliffe, 505 F.3d 944, 952 (9th Cir. 2007), found the Internet to be "similar to - and often using - our national network of telephone lines." It went on to conclude that:

> We have previously agreed that "[i]t can not be questioned that the nation's vast network of telephone lines constitutes interstate commerce," United States v. Holder, 302 F.Supp. 296, 298 (D. Mont. 1969)), aff'd and adopted, 427 F.2d 715 (9th Cir. 1970) (per curiam), and, a fortiori, it seems clear that use of the internet is intimately related to interstate commerce. As we have noted, "[t]he Internet engenders a medium of communication that enables information to be quickly, conveniently, and inexpensively disseminated to hundreds of millions of individuals worldwide." United States v. Pirello, 255 F.3d 728, 729 (9th Cir. 2001). It is "comparable . . . to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and

[13] As also stated in Senate Report No. 104-357, at 7 (1996), reprinted at 1996 WL 492169 (henceforth "S. Rep. No. 104-357"), ". . . the term 'obtaining information' includes merely reading it."

> services," ACLU, 521 U.S. at 853, and is "a valuable tool in today's commerce," Pirello, 255 F.3d at 730. We are therefore in agreement with the Eighth Circuit's conclusion that "[a]s both the means to engage in commerce and the method by which transactions occur, "the Internet is an instrumentality and channel of interstate commerce." United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (per curiam) (quoting United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006)).

Id. at 952-53. Thus, the third element is satisfied whenever a person using a computer contacts an Internet website and reads any response from that site.

As to the second element (i.e., that the accessing of the computer involve an interstate or foreign communication),[14] an initial question arises as to whether the communication itself must be interstate or foreign (i.e., it is transmitted across state lines or country borders) or whether it simply requires that the computer system, which is accessed for purposes of the communication, is interstate or foreign in nature (for example, akin to a national telephone system).[15] The term "interstate or foreign communication" is not defined in the CFAA. However, as observed in Patrick Patterson Custom Homes, Inc. v. Bach, 586 F.Supp.2d 1026, 1033 (N.D. Ill. 2008), "[t]he plain language of section 1030(a)(2)(C) requires that the conduct of unlawfully accessing a computer, and not the obtained information, must involve an interstate or foreign communication." See also Charles Schwab & Co. Inc. v. Carter, 2005 U.S. Dist. LEXIS 21348 at *26 (N.D. Ill. 2005). It has been held that "[a]s a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement." Paradigm Alliance, Inc. v. Celeritas Technologies, LLC, 248 F.R.D. 598, 602 (D. Kan. 2008); see also Patrick

---

[14] It is noted that, with the 2008 amendment to section 1030(a)(2)(C) which struck the provision that "the conduct involved an interstate or foreign communication" (see footnote 11, supra), the second element is no longer a requirement for the CFAA 18 U.S.C. § 1030(a)(2)(C) crime, although the interstate/foreign nexus remains as part of the third element.

[15] A resolution of that question would not effect Defendant's conviction here since the undisputed evidence at trial is that MySpace's server is connected to the Internet and the communications made by the alleged conspirators in O'Fallon, Missouri to Megan would automatically be routed to MySpace's server in Beverly Hills, California where it would be stored and thereafter sent to or retrieved by Megan in O'Fallon.

Patterson Custom Homes, 586 F.Supp.2d at 1033-34; Modis, Inc. v. Bardelli, 531 F.Supp.2d 314, 318-19 (D. Conn. 2008); Charles Schwab & Co., 2005 U.S. Dist. LEXIS 21348 at *26-27. This interpretation is consistent with the legislative history of the CFAA.[16] Therefore, where contact is made between an individual's computer and an Internet website, the second element is per se established.

As to the first element (i.e. intentionally accessing a computer without authorization or exceeding authorized access), the primary question here is whether any conscious violation of an Internet website's terms of service will cause an individual's contact with the website via computer to become "intentionally access[ing] . . . without authorization" or "exceeding authorization." Initially, it is noted that three of the key terms of the first element (i.e., "intentionally," "access a computer," and "without authorization") are undefined, and there is a considerable amount of controversy as to the meaning of the latter two phrases. See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."); Southwest Airlines Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 at *36 (N.D. Tex. 2007) ("BoardFirst") ("The CFAA does not define the term 'access'."); Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse

---

[16] For example, as stated in S. Rep. No. 104-357, at 13:

> The bill would amend subsection 1030(e)(2) by replacing the term "Federal interest computer" with the new term "protected computer" and a new definition . . . . The new definition also replaces the current limitation in subsection 1030(e)(2)(B) of "Federal interest computer" being "one of two or more computers used in committing the offense, not all of which are located in the same State." Instead, "protected computer" would include computers "used in interstate or foreign commerce or communications." Thus, hackers who steal information or computer usage from computers in their own State would be subject to this law, under amended section 1030(a)(4), if the requisite damage threshold is met and the computer is used in interstate commerce or foreign commerce or communications.

Statutes, 78 N.Y.U. L. Rev. 1596, 1619-21 (2003) ("Kerr, Cybercrime's Scope"); Mark A. Lemley, Place and Cyberspace, 91 Cal. L. Rev. 521, 528-29 (2003); Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 Cal. L. Rev. 439, 477 (2003).

While "intentionally" is undefined, the legislative history of the CFAA clearly evinces Congress's purpose in its choice of that word. Prior to 1986, 18 U.S.C. § 1030(a)(2) utilized the phrase "knowingly accesses." See United States Code 1982 Ed. Supp. III at 16-17. In the 1986 amendments to the statute, the word "intentionally" was substituted for the word "knowingly." See 18 U.S.C.A. § 1030 "Historical and Statutory Notes" at 450 (West 2000). In Senate Report No. 99-432 at 5-6, reprinted at 1986 U.S.C.C.A.N. 2479, 2483-84, it was stated that:

> Section 2(a)(1) amends 18 U.S.C. 1030(a)(2) to change the scienter requirement from "knowingly" to "intentionally," for two reasons. First, intentional acts of unauthorized access - rather than mistaken, inadvertent, or careless ones - are precisely what the Committee intends to proscribe. Second, the Committee is concerned that the "knowingly" standard in the existing statute might be inappropriate for cases involving computer technology . . . . The substitution of an "intentional" standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that "'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." [Footnote omitted.]

Under § 1030(a)(2)(C), the "requisite intent" is "to obtain unauthorized access of a protected computer." United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007) ("The government need not also prove that . . . the information was used to any particular ends."); see also S.Rep. No.104-357, at 7-8 ("[T]he crux of the offense under subsection 1030(a)(2)(C) . . . is abuse of a computer to obtain the information.").

As to the term "accesses a computer," one would think that the dictionary definition of verb transitive "access" would be sufficient. That definition is "to gain

or have access to; to retrieve data from, or add data to, a database . . . ." Webster's New World Dictionary, Third College Edition, 7 (1988) (henceforth "Webster's New World Dictionary"). Most courts that have actually considered the issue of the meaning of the word "access" in the CFAA have basically turned to the dictionary meaning. See e.g. BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *36; Role Models Am., Inc. v. Jones, 305 F. Supp. 2d 564, 566-57 (D. Md. 2004); Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F.Supp.2d 1255, 1272-73 (N.D. Iowa 2000). However, academic commentators have generally argued for a different interpretation of the word. For example, as stated in Patricia L. Bellia, Defending Cyberproperty, 79 N.Y.U. L. Rev. 2164, 2253-54 (2004):

> We can posit two possible readings of the term "access." First, it is possible to adopt a broad reading, under which "access" means any interaction between two computers. In other words, "accessing" a computer simply means transmitting electronic signals to a computer that the computer processes in some way. A narrower understanding of "access" would focus not merely on the successful exchange of electronic signals, but rather on conduct by which one is in a position to obtain privileges or information not available to the general public. The choice between these two meanings of "access" obviously affects what qualifies as unauthorized conduct. If we adopt the broader reading of access, and any successful interaction between computers qualifies, then breach of policies or contractual terms purporting to outline permissible uses of a system can constitute unauthorized access to the system. Under the narrower reading of access, however, only breach of a code-based restriction on the system would qualify.

Professor Bellia goes on to conclude that "[c]ourts would better serve both the statutory intent of the CFAA and public policy by limiting its application to unwanted uses only in connection with code-based controls on access." Id. at 2258. But see Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at 1619-21, 1643, and 1646-48 (arguing for a "broad construction of access . . . . as any successful interaction with the computer"). It is simply noted that, while defining "access" in terms of a code-based

restriction might arguably be a preferable approach, no case has adopted it[17] and the CFAA legislative history does not support it.

As to the term "without authorization," the courts that have considered the phrase have taken a number of different approaches in their analysis. See generally Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at 1628-40. Those approaches are usually based upon analogizing the concept of "without authorization" as to computers to a more familiar and mundane predicate presented in or suggested by the specific factual situation at hand. See e.g. United States v. Phillips, 477 F.3d 215, 219 (5th Cir.), cert. denied, 128 S.Ct. 119 (2007), ("Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."). Thus, for example, where a case arises in the context of employee misconduct, some courts have treated the issue as falling within an agency theory of authorization. See, e.g., International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1124-25 (W.D. Wash. 2000). Likewise, the Ninth Circuit (in dealing with the issue of purported consent to access emails pursuant to a subpoena obtained in bad faith in the context of the Stored Communications Act, 18 U.S.C. § 2701 et seq., and the CFAA) applied the law of trespass to determine whether a subpoenaed party had effectively authorized the defendants' access. See Theofel v. Farey-Jones, 359 F.3d 1066, 1072-75, 1078 (9th Cir. 2004). Further, where the relationship between the parties is contractual in nature or resembles such a relationship, access has been held to be unauthorized where there has been an ostensible breach of contract. See e.g., EF Cultural Travel BV, 274 F.3d at 583-84; Phillips, 477 F.3d at 221 ("[c]ourts have

---

[17] But see BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *43-44 ("§ 1030(a)(2)(C). However, the BoardFirst court did not adopt a "code-based" definition of "accessing without authorization" but requested further briefing on the issue.

recognized that authorized access typically arises only out of a contractual or agency relationship."). But see Brett Senior & Associates v. Fitzgerald, 2007 U.S. Dist. LEXIS 50833 at *13-14 (E.D. Pa. 2007) (observing - in the context of an employee's breach of a confidentiality agreement when he copied information from his firm's computer files to give to his new employer: "It is unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract.").

Within the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization. See, e.g., Southwest Airlines Co. v. Farechase, Inc., 318 F.Supp.2d 435, 439-40 (N.D. Tex. 2004); Nat'l Health Care Disc., Inc., 174 F.Supp.2d at 899; Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238, 247-51 (S.D.N.Y. 2000), aff'd, 356 F.3d 393 (2d Cir. 2004); Am. Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, 450 (E.D. Va. 1998); see also EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62-63 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access . . . . [W]e think that the public website provider can easily spell out explicitly what is forbidden . . . ."). But see BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *40 (noting that the above cases and their particular application of the law "have received their share of criticism from commentators"). The court in BoardFirst further stated:

> [I]t is at least arguable here that BoardFirst's access of the Southwest website is not at odds with the site's intended function; after all, the site is designed to allow users to obtain boarding passes for Southwest flights via the computer. In no sense can BoardFirst be considered an "outside hacker[] who break[s] into a computer" given that southwest.com is a publicly available website that anyone can access and use. True, the Terms posted on south-west.com do not give sanction to the particular *manner* in which BoardFirst uses the site -- to check in Southwest customers for financial gain. But then again § 1030 (a)(2)(C) does not forbid the *use* of a protected computer

> for any prohibited *purpose*; instead it prohibits one from intentionally *accessing* a computer "without authorization". As previously explained, the term "access", while not defined by the CFAA, ordinarily means the "freedom or ability to . . . make use of" something. Here BoardFirst or any other computer user obviously has the *ability* to make use of southwest.com given the fact that it is a publicly available website the access to which is not protected by any sort of code or password. *Cf.* Am. Online, 121 F.Supp.2d at 1273 (remarking that it is unclear whether an AOL member's violation of the AOL membership agreement results in "unauthorized access").[18]

Id. at 43-44 (emphasis in original).

In this particular case, as conceded by the Government,[19] the only basis for finding that Drew intentionally accessed MySpace's computer/servers without authorization and/or in excess of authorization was her and/or her co-conspirator's violations of the MSTOS by deliberately creating the false Josh Evans profile, posting a photograph of a juvenile without his permission and pretending to be a sixteen year old O'Fallon resident for the purpose of communicating with Megan. Therefore, if conscious violations of the MySpace terms of service were not sufficient to satisfy the first element of the CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(b)(2)(A), Drew's Rule 29(c) motion would have to be granted on that basis alone. However, this Court concludes that an intentional breach of the MSTOS can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute.

There is nothing in the way that the undefined words "authorization" and "authorized" are used in the CFAA (or from the CFAA's legislative history[20]) which

---

[18] Subsequently, the court in Am. Online did conclude that violating the website's terms of service would be sufficient to constitute "exceed[ing] authorized access." 174 F.Supp.2d at 899.

[19] See Reporter's Transcript of July 2, 2009 Hearing at 3-4.

[20] For example, when Congress added the term "exceeds authorized access" to the CFAA in 1986 and defined it as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter", it was observed that the definition (which includes the concept of accessing a computer with authorization) was "self-explanatory."

indicates that Congress intended for them to have specialized meanings.[21] As delineated in Webster's New World Dictionary at 92, to "authorize" ordinarily means "to give official approval to or permission for . . . ."

It cannot be considered a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website. See generally Phillips, 477 F.3d at 219-21; EF Cultural Travel BV, 318 F.3d at 62; Register.com, Inc., 126 F.Supp.2d at 245-46; CompuServe Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015, 1023-24 (S.D. Ohio 1997). Nor can it be doubted that the owner can relay and impose those limitations/restrictions/conditions by means of written notice such as terms of service or use provisions placed on the home page of the website. See EF Cultural Travel BV, 318 F.3d at 62-63. While issues might be raised in particular cases as to the sufficiency of the notice and/or sufficiency of the user's assent to the terms, see generally Specht v. Netscape Communications Corp., 306 F.3d 17, 30-35 (2d Cir. 2002); BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *11-21, and while public policy considerations might in turn limit enforcement of particular restrictions, see EF Cultural Travel BV, 318 F.3d at 62, the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.

Here, the MSTOS defined "services" as including "the MySpace.com Website . . . , the MySpace.com instant messenger, and any other connection with the Website . . . ." See Exhibit 3 at 1. It further notified the public that the MSTOS "sets forth the

---

See S.Rep. No. 99-432, at 13 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2491.

[21] Commentators have criticized the legislatures' understandings of computers and the accessing of computers as "simplistic" and based upon the technology in existence in the 1970's and 1980's (e.g. pre-Internet) rather than upon what currently exists. See, e.g., Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at 1640-41.

legally binding terms for your use of the services." Id. Visitors and members were informed that "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." Id. Moreover, to become a MySpace member and thereby be allowed to communicate with other members and fully utilize the MySpace Services, one had to click on a box to confirm that the user had agreed to the MySpace Terms of Service. Id.; see also Exhibit 1 at 2. Clearly, the MSTOS was capable of defining the scope of authorized access of visitors, members and/or users to the website.[22]

B. Contravention of the Void-for-Vagueness Doctrine

1. Applicable Law

Justice Holmes observed that, as to criminal statutes, there is a "fair warning"

---

[22] MySpace utilizes what have become known as "browsewrap" and "clickwrap" agreements in regards to its terms of service. Browsewraps can take various forms but basically the website will contain a notice that - by merely using the services of, obtaining information from, or initiating applications within the website - the user is agreeing to and is bound by the site's terms of service. See Burcham v. Expedia, Inc., 2009 U.S. Dist. LEXIS 17104 at *9-10 n.5 (E.D. Mo. 2009); BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *13-15; Ticketmaster Corp. v. Tickets.Com, Inc., 2003 U.S. Dist. LEXIS 6483 at * 9 (C.D. Cal. 2003) ("[A] contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases presumptive knowledge) of the conditions accepted when doing so."); Specht v. Netscape Communications Corp., 150 F.Supp.2d 585, 594 (S.D.N.Y. 2001), aff'd, 306 F.3d 17 (2d Cir. 2002); Pollstar v. Gigmania, Ltd., 170 F.Supp.2d 974, 981 (E.D. Cal. 2000). "Courts considering browsewrap agreements have held that 'the validity of a browsewrap license turns on whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site.'" Burcham, 2009 U.S. Dist. LEXIS 17104 at *9-10 n.5, quoting BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *15-16.

Clickwrap agreements require a user to affirmatively click a box on the website acknowledging awareness of and agreement to the terms of service before he or she is allowed to proceed with further utilization of the website. See Specht, 306 F.3d at 22 n.4; CoStar Realty Info., Inc. v. Field, 612 F.Supp.2d 660, 669 (D. Md. 2009). Clickwrap agreements "have been routinely upheld by circuit and district courts." Burcham, 2009 U.S. Dist. LEXIS 17104 at *8; see also Specht, 306 F.3d at 22 n.4; CoStar Realty Info., 612 F.Supp.2d at 669; DeJohn v. The .TV Corp. Int'l, 245 F.Supp.2d 913, 921 (N.D. Ill. 2003).

As a "visitor" to the MySpace website and being initially limited to the public areas of the site, one is bound by MySpace's browsewrap agreement. If one wishes further access into the site for purposes of creating a profile and contacting MySpace members (as Drew and the co-conspirators did), one would have to affirmatively acknowledge and assent to the terms of service by checking the designated box, thereby triggering the clickwrap agreement. As stated in the MSTOS, "This Agreement is accepted upon your use of the Website or any of the Services and is further affirmed by you becoming a Member." Exhibit 3 at 7; see generally, Doe v. MySpace, Inc., 474 F.Supp.2d 843, 846 (W.D. Tex. 2007).

requirement. As he stated in McBoyle v. United States, 283 U.S. 25, 27 (1931):

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.

As further elaborated by the Supreme Court in United States v. Lanier, 520 U.S. 259, 266 (1997):

> There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of "a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application." Connally v. General Constr. Co., 269 U.S. 385, 391 (1926) . . . . Second, as a sort of "junior version of the vagueness doctrine," H. Packer, The Limits of the Criminal Sanction 95 (1968), the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered . . . . Third, although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, . . . due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope. . . . In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal. [Citations omitted.]

The void-for-vagueness doctrine has two prongs: 1) a definitional/notice sufficiency requirement and, more importantly, 2) a guideline setting element to govern law enforcement. In Kolender v. Lawson, 461 U.S. 352, 357-58 (1983), the Court explained that:

> As generally stated, the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforce-ment . . . . Although the doctrine focuses both on actual notice to citizens and arbitrary enforcement, we have recognized recently that the more important aspect of the vagueness doctrine "is not actual notice, but the other principal element of the doctrine – the requirement that a legislature establish minimal guidelines to govern law enforcement."

> Smith [v. Goguen], 415 U.S. [566,] 574 [1974]. Where the legislature fails to provide such minimal guidelines, a criminal statute may permit "a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections." Id. at 575. [Footnote and citations omitted.]

To avoid contraving the void-for-vagueness doctrine, the criminal statute must contain "relatively clear guidelines as to prohibited conduct" and provide "objective criteria" to evaluate whether a crime has been committed. Gonzalez v. Carhart, 550 U.S. 124, 149 (2007) (quoting Posters 'N' Things, Ltd. v. United States, 511 U.S. 513, 525-26 (1994)). As stated in Connally v. General Construction Co., 269 U.S. 385, 391-92 (1926):

> The question whether given legislative enactments have been thus wanting in certainty has frequently been before this court. In some of the cases the statutes involved were upheld; in others, declared invalid. The precise point of differentiation in some instances is not easy of statement. But it will be enough for present purposes to say generally that the decisions of the court upholding statutes as sufficiently certain, rested upon the conclusion that they employed words or phrases having a technical or other special meaning, well enough known to enable those within their reach to correctly apply them, . . . or a well-settled common law meaning, notwithstanding an element of degree in the definition as to which estimates might differ, . . . or, as broadly stated . . . in United States v. Cohen Grocery Co., 255 U.S. 81, 92, "that, for reasons found to result either from the text of the statutes involved or the subjects with which they dealt, a standard of some sort was afforded." [Citations omitted.]

However, a "difficulty in determining whether certain marginal offenses are within the meaning of the language under attack as vague does not automatically render a statute unconstitutional for indefiniteness . . . . Impossible standards of specificity are not required." Jordan v. De George, 341 U.S. 223, 231 (1951) (citation and footnote omitted). "What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is." United States v. Williams, ___ U.S. ___, 128 S.Ct. 1830, 1846 (2008). In this regard, the Supreme Court "has made clear that scienter requirements alleviate vagueness concerns." Gonzales, 550

U.S. at 149; see also Colautti v. Franklin, 439 U.S. 379, 395 (1979) ("This Court has long recognized that the constitutionality of a vague statutory standard is closely related to whether that standard incorporates a requirement of *mens rea*").

"It is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in the light of the facts of the case at hand." United States v. Mazurie, 419 U.S. 544, 550 (1975); United States v. Purdy, 264 F.3d 809, 811 (9th Cir. 2001). "Whether a statute is . . . unconstitutionally vague is a question of law . . . ." United States v. Ninety-Five Firearms, 28 F.3d 940, 941 (9th Cir. 1994).

2. Definitional/Actual Notice Deficiencies

The pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies.

As discussed in Section IV(A) above, terms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of "common intelligence" are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not.

First, an initial inquiry is whether the statute, as it is written, provides sufficient notice. Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has "criminalized breaches of contract" in the context of website terms of service. Normally, breaches of contract are not the subject of criminal prosecution. See generally United States v. Handakes, 286 F.3d 92, 107 (2d Cir. 2002), overruled on other grounds in United States v. Rybicki, 354 F.3d 124, 144 (2d Cir. 2003) (en banc). Thus, while "ordinary people" might expect to be

exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties.[23] Id. This would especially be the case where the services provided by MySpace are in essence offered at no cost to the users and, hence, there is no specter of the users "defrauding" MySpace in any monetary sense.[24]

Second, if a website's terms of service controls what is "authorized" and what is "exceeding authorization" - which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. For example, in the present case, MySpace's terms of service prohibits a member from engaging in a multitude of activities on the website, including such conduct as "criminal or tortious activity," "gambling," "advertising to . . . any Member to buy or sell any products," "transmit[ting] any chain letters," "covering or obscuring the banner advertisements on your personal profile page," "disclosing your password to any third party," etc. See Exhibit 3 at 5. The MSTOS does not specify which precise terms of service, when breached, will result in a termination of MySpace's authorization for the visitor/member to access the website. If any violation of any term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-

---

[23] But see United States v. Sorich, 427 F.Supp.2d 820, 834 (N.D. Ill. 2006), aff'd, 531 F.3d 501 (7th Cir. 2008), cert. denied, 129 S.Ct. 1308 (2009) ("[S]imply because . . . actions can be considered violations of the 'contract' . . . does not mean that those same actions do not qualify as violations of [a criminal] statute.").

[24] Also, it is noted here that virtually all of the decisions which have found a breach of a website's terms of service to be a sufficient basis to establish a section 1030(a)(2)(C) violation have been in civil actions, not criminal cases.

for-vagueness doctrine as to setting guidelines to govern law enforcement.[25]

Third, by utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner - in essence - the party who ultimately defines the criminal conduct. This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers. For example, the MSTOS prohibits members from posting in "band and filmmaker profiles . . . sexually suggestive imagery or any other unfair . . . [c]ontent intended to draw traffic to the profile." Exhibit 3 at 4. It is unclear what "sexually suggestive imagery" and "unfair content"[26] mean. Moreover, website owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS provides that what constitutes "prohibited content" on the website is determined "in the sole discretion of MySpace.com . . . ." Id. Additionally, terms of service may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users. See, e.g., id. at 1.

Fourth, because terms of service are essentially a contractual means for setting the scope of authorized access, a level of indefiniteness arises from the necessary application of contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution. For example, the MSTOS has a provision wherein "any dispute" between MySpace and a visitor/member/user arising out of the terms of service is subject to arbitration upon the demand of either party. Before a breach of a term of service can be found and/or the effect of that breach upon MySpace's ability to terminate the visitor/member/user's access to the

---

[25] Another uncertainty is whether, once a user breaches a term of service, is every subsequent accessing of the website by him or her without authorization or in excess of authorization.

[26] See Time Warner Entm't Co., L.P. v. FCC, 240 F.3d 1126, 1135 (D.C. Cir. 2001) ("The word 'unfair' is of course extremely vague.").

site can be determined, the issue would be subject to arbitration.[27] Thus, a question arises as to whether a finding of unauthorized access or in excess of authorized access can be made without arbitration.

Furthermore, under California law,[28] a material breach of the MSTOS by a user/member does not automatically discharge the contract, but merely "excuses the injured party's performance, and gives him or her the election of certain remedies." 1 Witkin, Summary of California Law (Tenth Ed.): Contracts § 853 at 940 (2008). Those remedies include rescission and restitution, damages, specific performance, injunction, declaratory relief, etc. Id. The contract can also specify particular remedies and consequences in the event of a breach which are in addition to or a substitution for those otherwise afforded by law. Id. at § 855 at 942. The MSTOS does provide that: "MySpace.com reserves the right, in its sole discretion . . . to restrict, suspend, or terminate your access to all or part of the services at any time, for any or no reason, with or without prior notice, and without liability." Exhibit 3 at 2. However, there is no provision which expressly states that a breach of the MSTOS automatically results in the termination of authorization to access the website. Indeed, the MSTOS cryptically states: "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." Id. at 1 (emphasis

---

[27] An arbitration clause is considered to be "broad" when it contains language to the effect that arbitration is required for "any" claim or dispute which "arises out of" the agreement. Fleet Tire Service v. Oliver Rubber Co., 118 F.3d 619, 621 (8th Cir. 1997); see also Schoenduve Corp. v. Lucent Technologies, Inc., 442 F.3d 727, 729 (9th Cir. 2006). Where a broad arbitration clause is in effect, "even the question of whether the controversy relates to the agreement containing the clause is subject to arbitration." Fleet Tire Service, 118 F.3d at 621. Moreover, "[a]n agreement to arbitrate 'any dispute' without strong limiting or excepting language immediately following it logically includes not only the dispute, but the consequences naturally flowing from it . . . ." Management & Tech. Consultants v. Parsons-Jurden, 820 F.2d 1531, 1534-35 (9th Cir. 1987). Further, where the parties have agreed that an issue is to be resolved by way of arbitration, the matter must be decided by the arbitrator, and "a court is not to rule on the potential merits of the underlying claim[] . . . . indeed even if it appears to the court to be frivolous . . . ." AT&T Technologies, Inc. v. Communications Workers of Am., 475 U.S. 643, 649-50 (1986).

[28] According to the MSTOS, "If there is any dispute about or involving the Services, you agree that the dispute shall be governed by the laws of the State of California without regard to conflict of law provisions . . . ." Exhibit 3 at 7.

added).

3. The Absence of Minimal Guidelines to Govern Law Enforcement

Treating a violation of a website's terms of service, without more, to be sufficient to constitute "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals. As noted in Section IV(A) above, utilizing a computer to contact an Internet website by itself will automatically satisfy all remaining elements of the misdemeanor crime in 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A). Where the website's terms of use only authorizes utilization of its services/applications upon agreement to abide by those terms (as, for example, the MSTOS does herein), any violation of any such provision can serve as a basis for finding access unauthorized and/or in excess of authorization.

One need only look to the MSTOS terms of service to see the expansive and elaborate scope of such provisions whose breach engenders the potential for criminal prosecution. Obvious examples of such breadth would include: 1) the lonely-heart who submits intentionally inaccurate data about his or her age, height and/or physical appearance, which contravenes the MSTOS prohibition against providing "information that you know is false or misleading"; 2) the student who posts candid photographs of classmates without their permission, which breaches the MSTOS provision covering "a photograph of another person that you have posted without that person's consent"; and/or 3) the exasperated parent who sends out a group message to neighborhood friends entreating them to purchase his or her daughter's girl scout cookies, which transgresses the MSTOS rule against "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services." See Exhibit 3 at 4. However, one need not consider hypotheticals to demonstrate the problem. In this case, Megan (who was then 13 years old) had her own profile on MySpace, which was in clear violation of the MSTOS which requires that users be

"14 years of age or older." Id. at 2. No one would seriously suggest that Megan's conduct was criminal or should be subject to criminal prosecution.

Given the incredibly broad sweep of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A), should conscious violations of a website's terms of service be deemed sufficient by themselves to constitute accessing without authorization or exceeding authorized access, the question arises as to whether Congress has "establish[ed] minimal guidelines to govern law enforcement." Kolender, 461 U.S. at 358; see also City of Chicago v. Morales, 527 U.S. 41, 60 (1999). Section 1030(a)(2)(C) does not set forth "clear guidelines" or "objective criteria" as to the prohibited conduct in the Internet/website or similar contexts. See generally Posters 'N' Things, Ltd., 511 U.S. at 525-26. For instance, section 1030(a)(2)(C) is not limited to instances where the website owner contacts law enforcement to complain about an individual's unauthorized access or exceeding permitted access on the site.[29] Nor is there any requirement that there be any actual loss or damage suffered by the website or that there be a violation of privacy interests.

The Government argues that section 1030(a)(2)(C) has a scienter requirement which dispels any definitional vagueness and/or dearth of guidelines, citing to United States v. Sablan, 92 F.3d 865 (9th Cir. 1996). The Court in Sablan did observe that:

> [T]he computer fraud statute does not criminalize otherwise innocent conduct. Under the statute, the Government must prove that the defendant intentionally accessed a federal interest computer without authorization. Thus, Sablan must have had a wrongful intent in accessing the computer in order to be convicted under the statute. This case does not present the prospect of a defendant being convicted without any wrongful intent as was the situation in [United States v.] X-Citement Video [513 U.S. 64, 71-73 (1994)].

Id. at 869. However, Sablan is easily distinguishable from the present case as it: 1)

[29] Here, the prosecution was not initiated based on a complaint or notification from MySpace to law enforcement officials.

did not involve the defendant's accessing an Internet website;[30] 2) did not consider the void-for-vagueness doctrine but rather the *mens rea* requirement; and 3) dealt with a different CFAA subsection (i.e. 18 U.S.C. § 1030(a)(5)) and in a felony situation.

The only scienter element in section 1030(a)(2)(C) is the requirement that the person must "intentionally" access a computer without authorization or "intentionally" exceed authorized access. It has been observed that the term "intentionally" itself can be vague in a particular statutory context. See, e.g., American Civil Liberties Union v. Gonzales, 478 F.Supp.2d 775, 816-17 (E.D. Pa. 2007), aff'd, 534 F.3d 181, 205 (3rd Cir. 2008), cert. denied, 129 S.Ct. 1032 (2009).

Here, the Government's position is that the "intentional" requirement is met simply by a conscious violation of a website's terms of service. The problem with that view is that it basically eliminates any limiting and/or guiding effect of the scienter element. It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization. This is especially the case with MySpace and similar Internet venues which are publically available for access and use. See generally BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *43. However, if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution. All manner of situations will be covered from the more serious (e.g. posting child pornography) to the more trivial (e.g. posting a picture of friends without their permission). All can be prosecuted. Given the "standardless sweep" that results, federal law enforcement

[30] In Sablan, the defendant was a bank employee who had been recently fired for circumventing its security procedures in retrieving files. Early one morning, she entered the closed bank through an unlocked door and, using an unreturned key, went to her former work site. Utilizing an old password, she logged onto the bank's mainframe where she called up several computer files. Although defendant denied any additional actions, the government charged her with changing certain files and deleting others. As a result of her conduct, several bank files were severely damaged. See 92 F.3d at 866.

entities would be improperly free "to pursue their personal predilections."[31] Kolender, 461 U.S. at 358 (citing Smith v. Goguen, 415 U.S. 566, 575 (1994)).

In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]." City of Chicago, 527 U.S. at 64.

V. CONCLUSION

For the reasons stated above, the Defendant's motion under F.R.Crim.P. 29(c) is GRANTED.

DATED: This 28th day of August, 2009

GEORGE H. WU
United States District Judge

[31] In comparison, the felony violation of 18 U.S.C. § 1030(a)(2)(C) contains effective scienter elements because it not only requires the intentional accessing of a computer without authorization or in excess of authorization, but also the prerequisite that such access must be "in furtherance" of a crime or tortious act which, in turn, will normally contain additional scienter and/or wrongful intent conditions.